

PRODUCT AUTHENTICATION SYSTEM AND MERCHANDISE TAG TO BE USED FOR THE SAME SYSTEM

X1

Publication number: JP2000011114 (A)

Publication date: 2000-01-14

Inventor(s): KIKUCHI YOSHITOMO; TSUCHIDA TOSHIKATSU +

Applicant(s): HITACHI LTD +

Classification:

- international: G06K17/00; G06K19/07; G06Q10/00; G06Q30/00; G06Q50/00; G09C1/00;
H04L9/22; G06K17/00; G06K19/07; G06Q10/00; G06Q30/00; G06Q50/00;
G09C1/00; H04L9/32; (IPC1-7): G06F17/60; G06K17/00; G06K19/07; G09C1/00;
H04L9/32

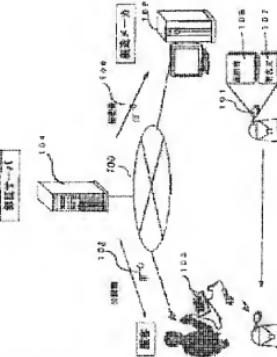
- European:

Application number: JP19980175500 19980 623

Priority number(s): JP19980175500 19980 623

Abstract of JP 2000011114 (A)

PROBLEM TO BE SOLVED: To provide a system for confirming whether or not a product is real or a fake by allowing a manufacturer/maker to record certificate data in the memory of a merchandise tag while adding an electric signature to the certificate data, and to ship the merchandise tag with this tag to the product, and allowing a purchaser to read this certificate data by an exclusive reader in a shop. **SOLUTION:** At the time of shipping a product, a merchandise tag 101 in which certificate data for certifying the manufacturer of the product by the maker are recorded is issued by a merchandise tag issuing means 102. The product is shipped after attaching the merchandise tag to the product. A purchaser in a shop reads and confirms the certificate from the merchandise tag 101 by a merchandise tag reading terminal 103. The purchaser of the product previously inputs the certificate decoding information from a certification server 104 through a network and mailing or the like to the reading terminal 103, and collates the certificate information of the merchandise tag 101 in the shop for confirming whether the product is real or a fake.

Data supplied from the **espacenet** database — Worldwide

【特許請求の範囲】

【請求項1】 秘密鍵と公開鍵を生成し管理する認証サーバと、該認証サーバで生成した秘密鍵を用いて製品の出所または品質を証明する証明書から電子署名を生成し、該証明書と該電子署名を、電子的なメモリを有する商品タグに書込んで発行する商品タグの発行機と、前記認証サーバで生成した公開鍵を用いて前記商品タグから読み取った証明書の真偽を確認する読取端末を有することを特徴とする製品認証システム。

【請求項2】 請求項1記載の製品認証システムにおいて、

前記読取端末は、前記証明書をハッシュ化して生成した第1のダイジェストメッセージと公開鍵で電子署名を復号化して生成した第2のダイジェストメッセージとを比較して証明書の真偽を判定することを特徴とする製品認証システム。

【請求項3】 製品認証システムに用いる商品タグであって、少なくとも証明書またはハッシュ化された電子署名を含む製品認証のための情報を内蔵メモリに記憶したことを特徴とする非接触式ICカードからなる商品タグ。

【請求項4】 請求項3記載の商品タグであって、

該商品タグを製品に連結するための紐の内部に、当該商品タグを構成する非接触式ICカードの配線の一部を内蔵することを特徴とする商品タグ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、物品の製品認証(真偽判定)に關し、特に、改竄や製品偽造が防止でき、製造メーカーを保護するために有効な製品認証システムおよびそれに用いる商品タグに関する。

【0002】

【従来の技術】 従来、商品の製造元や販売元は消費者に対してその商品の出所や品質を保証するために、商品の製品認証(出所や品質内容の認証)のための証明書を発行していた。その場合の証明書は、紙や布などを用い、署名として印鑑やサインなどが行われるのが普通であった。そのため、簡単に証明書を偽造することが可能であった。この偽造に対する従来の対策としては、透かしやホログラムなどを用いることにより偽造にくくする方法が講じられていた。

【0003】 また、インターネット上の公開鍵方式による本人認証の技術としては、RSA(Rivest Shamir Adleman)暗号化方式を用いる方法などが知られているが、本発明に関連するタグの特許としては、以下のものが挙げられる。特開平9-050501号公報(タグ)、特開平8-335257号公報(非接触:ICタグ)、特開平8-133424号公報(物品の管理方法、管理システム及びそれに適用されるタグ)。

【0004】

【発明が解決しようとする課題】かかる従来の方法においては、以下のような課題がある。上述したように、ブランド品などの商品に対して製造元(販売元)が出所や内容を証明する証明書は、従来、紙や布などによる表示で行っていて偽造や改竄が容易にできるため、偽造品が市場に氾濫しているのが現状である。このような現状において、製造元(販売元)の利益が侵害され購入者の製品に対する信頼感・安心感が低下し、社会問題化している。また、従来の証明書では偽造や改竄を防止するため透かしやホログラムなどの対策を講じていることが購入者に徹底されなければ、購入者が真偽判定することには困難であるという問題がある。本発明の目的は、上述の問題点を解決し、製品証明書の改竄、製品偽造を防止し、店舗、購入者の製品に対する信頼性の向上を図り、安心感を与えることができるだけでなく、流通段階、税関などにおいても商品の真偽判定ができる、製造メーカーの利益を保護する事が可能な製品認証システムおよびそれに用いられる商品タグを提供することである。

【0005】

【課題を解決するための手段】 本発明は、上記目的を達成するために、秘密鍵(106)と公開鍵(108)を生成し管理する認証サーバ(104)と、該認証サーバ(104)で生成した秘密鍵(106)を用いて製品の出所または品質を証明する証明書(105)から電子署名(107)を生成し、該証明書(105)と該電子署名(107)を、電子的なメモリを有する商品タグ(101)に書込んで発行する商品タグの発行機(102)と、前記認証サーバ(104)で生成した公開鍵(108)を用いて前記商品タグから読み取った証明書の真偽を確認する読取端末(103)を有することを特徴としている。さらに具体的には、読取端末(103)は、証明書をハッシュ化して生成した第1のダイジェストメッセージと公開鍵で電子署名を復号化して生成した第2のダイジェストメッセージを比較して証明書の真偽を判定することを特徴としている。また、本発明の商品タグは、証明書またはハッシュ化された電子署名を含む製品認証のための情報を内蔵メモリに記憶したものであり、さらに、該商品タグを製品に連結するための紐の内部に、当該商品タグを構成する非接触式ICカードの配線の一部(図2の201)を内蔵することを特徴としている。

【0006】

【発明の実施の形態】 以下、本発明の実施の形態について、図面を用いて説明する。図1は、本発明の全体システムの概念を示す図である。同図において、1001はネットワーク、101は製造メーカーが製品につける商品タグ(例えば非接触ICタグ)、102は商品タグ発行機、103は購入者が店舗で読み取りに用いる読取端末(商品タグリーダー)、104は認証サーバ、105は出

所や商品品質を証明する証明書、106は秘密鍵、107は電子署名、108は公開鍵である。

【0007】認証サーバ104は、秘密鍵と公開鍵の生成と管理を行っている。商品タグ発行機102は、ネットワーク100を介して認証サーバ104から秘密鍵106を受け取り、証明書の生成、証明書のハッシュ化による電子署名の生成、商品タグ101への証明書および電子署名の書き込み、および商品タグ101の発行を行うものである。読取端末103は、商品タグリーダー、携帯PCで構成されており、ネットワーク100を介して認証サーバ104から受け取った公開鍵108を用いて、読取端末103で商品タグ101から読み取った証明書および電子署名を照合することにより商品認証を行うものである。

【0008】図2は、本発明の商品タグ101を非接触ICカードを用いて構成した場合の構造例である。本商品タグ101は、アンテナ部201、メモリ機能を持つICチップ202で構成されている。通常の非接触ICタグの配線パターンの一部（電気的に接続されている部分であれば何れの部分であってもよいが、例えばアンテナ部201）をタグの紐となる部分の内部に往復するように内蔵させ、製品に取り付ける際に、タグの穴を通して紐の端に樹脂などでストッパー203で封止する。本構造を採用すると、封止後に商品タグを商品から外すためには配線パターンの一部（例えば、アンテナ210）となっている紐を切らねばならず、商品タグ101を商品から外すと同時に商品タグの機能は回路的に破壊され、無効となってしまうため一度商品から外した商品タグは再使用することができず、結果的に商品タグの再使用による悪用を防止することが可能となる。

【0009】次に、商品タグ発行機102の動作を説明する。図3は、商品タグ発行機102の動作フローチャートである。同図に示すように、まず、証明書（本文）を生成する（ステップ301）。次に、証明書をハッシュ化してダイジェストを作成した後、ネットワーク100を介して認証サーバ104から受け取った秘密鍵106で暗号化して電子署名を生成する（ステップ302）。次に、商品タグ101と通信を開始し（ステップ303）、前記生成した証明書（本文）と電子署名を商品タグのメモリ内へ書き込む（ステップ304）。

【0010】次に、読取端末103の動作を説明する。図4は、読取端末103の動作フローチャートである。同図は既にネットワーク100を介して認証サーバ104の公開鍵108を入手した後の動作を示している。まず、読取端末103は、商品タグ101との通信を開始し（ステップ401）、商品タグ101のメモリ内に格納されている証明書と電子署名を読取端末103へ読み込む（ステップ402）。次に、証明書（本文）をハッシュ化して第1のダイジェストメッセージAを作成する（ステップ403）。さらに、電子署名を公開鍵を用い

て復号化し第2のダイジェストメッセージ（ダイジェストメッセージB）を作成する（ステップ404）。この第1のダイジェストメッセージAと第2のダイジェストメッセージBを比較して一致するか判断する（ステップ405）。一致すれば本物であることを読取端末103の表示部に表示し（ステップ406）、もし一致しなければ、偽造品であることを同じく読取端末103の表示部に表示する（ステップ407）。

【0011】図5は、秘密鍵／公開鍵を用いた認証アルゴリズムを説明するための模式図である。以下、図3と図4の各ステップと対応付けて該認証アルゴリズムを説明する。商品タグ発行機102は、まず、（イ）証明書を生成し（図3のステップ301）、（ロ）証明書をハッシュすることによりダイジェストを作成し、（ハ）該ダイジェストメッセージを秘密鍵106で暗号化して電子署名を生成する（図3ステップ302）。（ニ）証明書と電子署名を商品タグ101のメモリ内に書き込む（図3ステップ303、304）。（ホ）商品タグ101から証明書と電子署名を読み出し（図4のステップ401～402）、証明書をハッシュして第1のダイジェストメッセージAを作成するとともに（図4ステップ403）、（ヘ）電子署名を公開鍵108で復号化し第2のダイジェストメッセージBを作成し（図4ステップ404）、（ト）該作成した第1のダイジェストメッセージAと第2のダイジェストメッセージBを比較し、その一致／不一致によって本物／偽物を判別する（図4ステップ405～407）。

【0012】上述した実施例では、秘密鍵106と公開鍵108の受け渡しをネットワーク100を介して実施する例を説明したが、これに限定せず、紙、フロッピーディスク（FD）、メモリカード、ICカード、CD-ROM、光磁気ディスク、DVDなどの記録媒体を用いて直接の手渡しや、郵送によるオンラインの受け渡しであってもよい。さらに、上述した実施例では、商品タグ101に記録する内容として証明書と電子署名の例を説明したが、その他の例として、①証明書のみ、②証明書+暗号化された証明書、③暗号化された証明書のみであってもよい。さらに、上述した実施例では、本発明の活用場所として、購入者が店舗にて活用する例を説明したが、製造メーカーから卸店へ卸す過程や卸店から小売店舗などに卸す過程などの各種流通過程、または税関などにおいても本発明が活用できることはいうまでもない。

【0013】

【発明の効果】以上説明したように、本発明によれば、製品認証商品タグによって、製品証明書の改竄、製品偽造を防止し、製造メーカーの利益を保護できる。また、読取端末により容易に商品の真偽判定が容易に行える。これにより店舗、購入者の製品に対する信頼性の向上を図り、安心感を与えることができるだけでなく、流通段階、税関などにおいても商品の真偽判定ができるなどの

優れた効果が奏される。

【図面の簡単な説明】

【図1】全体システムを示す図である。

【図2】商品タグの構造を示す図である。

【図3】商品タグ発行機の動作を示すフローチャートである。

【図4】読み取端末の動作を示すフローチャートである。

【図5】秘密鍵／公開鍵を用いた認証アルゴリズムを説明するための模式図である。

【符号の説明】

101：商品タグ

102：商品タグ発行機

103：読み取端末

104：認証サーバ

105：証明書（本文）

106：秘密鍵

107：電子署名

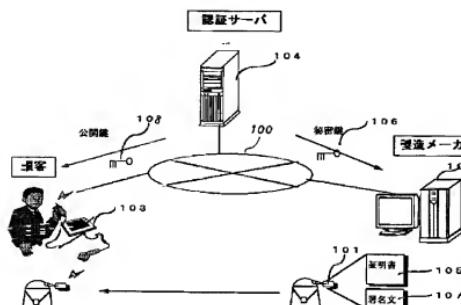
108：公開鍵

201：商品タグの配線パターンの一部（例：アンテナ）

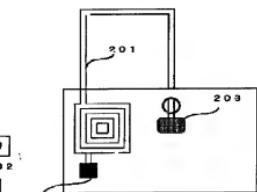
202：非接触ICタグ内部のICチップ

203：商品タグのストッパー（封止）

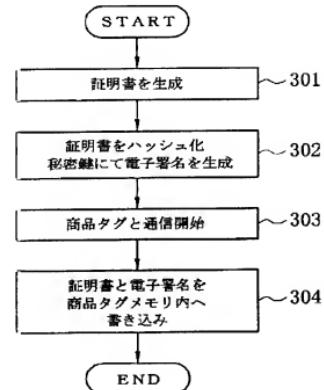
【図1】



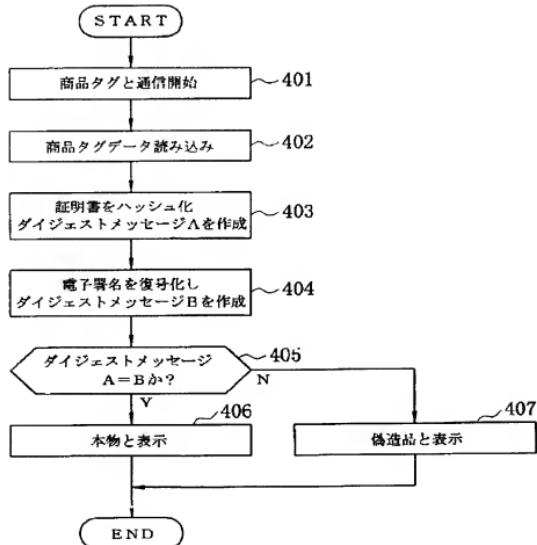
【図2】



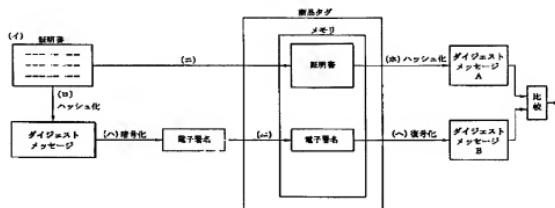
【図3】



【図4】



【図5】



フロントページの続き

Fターム(参考) 5B035 AA14 CA23 CA38
5B049 BB11 CC23 CC28 DD04 EE03
EE09 EE23 FF03 FF04 FF08
GG04 GG07 GG10
5B058 CA27 KA06 KA32 KA35
5K013 BA02 FA03 GA00 GA08